Secured Connection in Wireless AD-HOC Network With Multiple Relay Transmission Using Dynamic Source Routing Algorithm

R. Venkatesharjun[1] P. Bright Prabahar[2]
PG Student[1], Assistant Professor[2]
Department Of Electronics and Communication Engineering
Parisutham Institute of Technology & science
Thanjavur, Tamilnadu

Abstract --- **One of the decentralized types of wireless networks is a wireless ad hoc network (WANET). The network is so called as it does not rely on a pre-existing model, such as routers in the wired networks or AccessPoint(AP) in managed (infrastructure based) wireless networks. Instead, each of the nodes participates in routing by forwarding data to other nodes. In addition to the conventional routing, ad hoc networks use flooding for forwarding data. Here, we propose a wireless ad-hoc network with randomly generated eavesdroppers for analyzing the secrecy of connection between source and destination, in which we use dynamic source routing techniques to transfer the data between the source and destination nodes through the relay nodes.**

Keywords*– *Ad-Hoc Network, Relay Transmission, Dynamic Source Routing

I. INTRODUCTION

Relay networks consistingof Source (*S*), Several relays, Destination (*D*), and ofcourse number of eavesdroppers. All the nodes are equipped with one antenna. The distribution of relays and eavesdroppers are homogenous. We try to address the question of whether to use relay transmission in wireless ad hoc networksfrom a secure connectivity perspective or not. We considerthat the locations of both the potential relays and maliciouseavesdroppers are random following homogenous Poison point process (PPP)in wireless ad hoc networks based on the transmission range of base station. Here, the data transmission can be categorized asdirect transmission and Relay transmission.

A. Direct Transmission

If the distance between the source and destination is within the transmission range (or) the coverage range of the base station in WANET, then we go for direct transmission, in which the data should be shared between source and destination directly. That is,there is no intermediate node between source and destination.

B. Relay Transmission

The distance between the source and destination is large when compared with the transmission range of the base station. The data to be shared between the source and destination traverses the intermediate node(s). This type of transmission is called as relay transmission and the message forwarded through relay nodes is called as Hub-by-Hub message transmission.

II. RELATED WORK

A. The Relay-Eavesdropper Channel: Cooperation for Secrecy

This paper establishes the utility of user cooperation in facilitating secure wireless mode of communication. Particularly, the four-terminal relay hacker channel is introduced and an outer-bound on the optimal rate-equivocation region is found to be derived. Several cooperation strategies are devised and the corresponding achievable rate-equivocation region are characterized.The strategy of interest is the novel Noise-Forwarding (NF) strategy.

The main idea is to exploit user cooperation in facilitating the transmission of confidential messages from the source to the destination. The NF scheme transforms the relay-eavesdropper channel into a compound multiple access channel (MAC), where the source/relay to the receiver is the first MAC and source/relay to the eavesdropper is the second one. R1 is the codeword rate of the source, and R2 is the codeword rate of the relay. If the relay node does not transmit, the perfect secrecy rate is zero for the input distribution since R1(A) < R1(B). On the other hand, if the relay and the source coordinate their transmissions, we can also achieve equivocation rate (Re), which is strictly greater than zero. We can still get a positive perfect secrecy rate by operating at point A in the absence of relay. It is possible to get a larger secrecy rate by moving the operating point to B

Merits:

- ✓ Multi relay transmission
- ✓ Relaying gives more secure connection

Drawback:

- ✓ Unsecured eavesdropper networks.

B. Secrecy in Cooperative Relay Broadcast Channels

This paper investigates the effects of user cooperation on the secrecy of broadcast channels by considering a cooperative relay broadcast channel. We propose an achievable scheme that combines Marton's coding scheme for broadcast channels and Cover and El Gamal's compress-and-forward scheme for the relay channel. Wemay derive outer bounds for rate-equivocation region using auxiliary random variables for single-letterization. Finally, the Gaussian CRBC show that both users can have positive secrecy rates, which are not possible by scalar Gaussian broadcast channels without cooperation. To obtain positive secrecy rates for both of the users, we provide different assignment for auxiliary random variables appearing in achievable rate. This auxiliary random variable assignmentsmay have dirty paper coding (DPC) interpretations. In addition, we combine jamming and relaying to provide secrecy for both users when the relaying user is weak.

Merits:

- ✓ Avoids the collision attack.
- ✓ Reduces time delay.

Drawback

- ✓ Absence of access point and Storage mode may led to privacy problem

C. Characterization of the Secrecy Region of a Single Relay Cooperative System

This paper proposes how a simple cooperative network with one relaynode can improve the physical layer security by decreasing thearea in which the eavesdropper can reside and listen to theinformation transmitted to the destination. That region is calledvulnerability region. Undercertain conditions, the vulnerability region may vanish, which makesour wireless system perfectly secure for any position of theeavesdropper within the wireless network.

We characterize the vulnerability region in a single relay cooperative wireless network. Cooperation improves the physical layer security in the network by minimizing the area in which the secrecy capacity is zero. We realize that under certain conditions, vulnerability region, vanishes. In other words, for this case, we may have a perfectly secured system and no matter where the eavesdroppers reside, they will not be able to receive any information intended to the desired destination. This will be possible by carefully designed codes that achieve the secrecy capacity and *without* any key exchange. The improvement in the security is achieved by increasing the capacity of the direct channel by the help of relay, as well as by decreasing the capacity of eavesdropper channel by introducing interference (jamming) from the relay and the source.

Merit:

- ✓ Secure data transmission in single relay.

Drawbacks:

- ✓ Time delay.
- ✓ More complex networks.

D. The Effect of Eavesdroppers on Network ***Connectivity: A Secrecy Graph Approach***

This paper investigates the effect of eavesdroppers on thenetwork connectivity, by using wiretap module and Percolation theory. This wiretap module captures the effect of the eavesdroppers on the link security. A link is found to exist between two nodes, only if secrecy capacity of that particular link is positive. The percolation threshold is the critical value of probability of occurrence of an eavesdropper, above which an infinite connected component does not exist in the secrecy graph, almost surely.

Network connectivity is defined in the Percolation sense, that is the connectivity exists, if infinite connected component exists in the corresponding *Secrecy graph*. We may consider uncertainty in the location of eavesdroppers, modeled directly on the *network level* as correlated failures in the secrecy graph. Here, our approach attempts to bridge the gap between physical layer security under uncertain channel state information and network level connectivity under secrecy constraints. Both analytic and simulation results show that uncertainty in location of eavesdroppers has a dramatic effect on network connectivity in a secrecy graph.Thus, this paper provides bounds on percolation threshold for square and triangular lattices, which provide insight into the effect of uncertainty in eavesdropper's location on the percolation properties of lattice secrecy graphs.

Merit:

- ✓ Multiple data transmission

Drawback:

- ✓ Data loss in intermediate nodes

E. Towards Achieving Full Secrecy Rate in Wireless Networks: A Control Theoretic Approach

In this paper, we may consider a single-user secured data communication system. Data packets which arrives at the transmitter are to be enqueued at a data queue to be transmitted to the receiver over a block of fading channel, in a secure way from the eavesdropper that listen to the transmitter over an another independent block of fading channel. We address two individual problems, which involves the maximization of a long-term average utility, which is defined as a function of number of secured packets transmitted in every time slot. So, we propose a transmission controller and an admission controller based on simple index policies that do not rely on any prior statistical information on the process of data arrival. The former one chooses the random key generation (and transmission) rate as well as the secure data transmission rate in every time slot. The part of data is been secured by the available secrecy rate while the other part is encrypted by using key bits, which is enqueued at both the transmitter and at the receiver. The latter one chooses the amount of data which is admitted by the transmitter to be enqueued in data queue. We also show that our controller pair has a provable efficient performance. To our best knowledge, this is the first work that addresses the queuing delay in the context of secrecy.

- ✓ **Merit:**Data is more secure
- ✓ **Drawback:** Queuing delay in data packet.

III. EFFECTIVE CANCELLATION OF EAVESDROPPERS EFFECT ON NETWORK CONNECTIVITY USING RELAY TRANMISSION

Dynamic Source Routing (DSR) Techniques is used to transfer the Hub-by-Hub message transfer from Source to Destination through arbitrary relay nodes. The DSR protocol should connect the relay nodes between source and destination on Dynamic Routing strategies.DSR should select the relay node(s) based on the transmission range of base station which is chosen by the user.

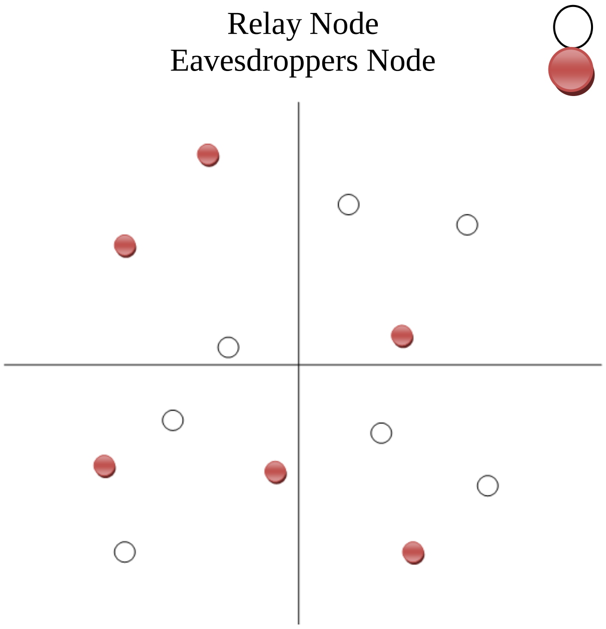
Network connectivity is defined in percolationsense, that is the connectivity exists if an infinite connected component is found to be exist in the corresponding *Secrecy Graph*. We mustconsider the uncertainty in thelocation of eavesdroppers, which is directlydesigned at the *Network level* as correlated failures in Secrecy graph. Our approach is here to attempt bridge gap between physical layer security under uncertain channel state information and network level connectivity under secrecy constraints. Both analytic and simulation results show that uncertainty in location of eavesdroppers has a dramatic effect on network connectivity in a secrecy graph.

The percolation threshold is the critical value of probability of occurrence of an eavesdropper, above which an infinite connected component does not exist in the secrecy graph, almost surely. Hence, this paper provides bounds on percolation threshold for square and triangular lattices, which provide insight into the effect of uncertainty in eavesdropper's location on the percolation properties of lattice secrecy graphs.

4. PROPOSED SYSTEM

Our proposed system implements the wireless ad hoc network with 'n' number of nodes that should construct the network for data transmission from one location to another. Each node is having the unique id and its related locations. The randomly generated eavesdropping nodes are also present with in this network. The nodes are moving with static velocity and also the moving position of the each node is mentioned with (x, y) co-ordinates. Then the network should establish the connection with base station. Then the user should select the source, destination node and message and transmission range of the base station. If the distance between the source and destination is within the transmission range the direct data transmission is possible otherwise the transmission is relay transmission. i.e. The message forwarded between the relay nodes, in which the relay nodes are either original nodes or eavesdroppers. In this situation we can analyze the security of the connection and overall efficiency of the network.

A. SYSTEM MODEL



We consider a relay network consisting of one source (*S*), several relays (*Rl* , *l* = 1, 2, . . .), one destination (*D*), and several eavesdroppers (*E j* , *j* = 1, 2, . . .). All the nodes are equipped with one antenna. The distance between the source and destination is equal to d_{SD}. The distributions of relays and eavesdroppers are homogenous PPPs $\Phi_R$and $\Phi_E$with density $\lambda_R$and λ_E, respectively. In this system, all the transmitters transmit with the same power. Then we can obtain the instantaneous signal-to-noise ratio (SNR) at the relays, destination, and eavesdroppers as

$$\boldsymbol{SNR_{nm}= \varepsilon h_{nm} d_{nm}}^{-\alpha}$$

Whereε→transmits SNR

$\boldsymbol{h_{nm}}$→small-scale fading (follows exponential distribution with unit mean)

$\boldsymbol{d_{mn}}$=||$\boldsymbol{x_m}$−$\boldsymbol{x_n}$||→ Euclidean distance between node *n* and node *m* mean

$\boldsymbol{x_n}$→ location of node *n*.

$\boldsymbol{\alpha}$→ path-loss exponent

The relay transmission is not necessary if the direct transmission is strong enough. According to d_{SD}, we can know how strong the direct transmission is. For colluding eavesdroppers, to avoid relaying for the users having strong direct transmission we define a target secure connection probability δ constraint for direct transmission. Assume eavesdroppers cannot be allowed to collude and exchange information. The secure performance is determined with the strongest received signal from the transmitter.

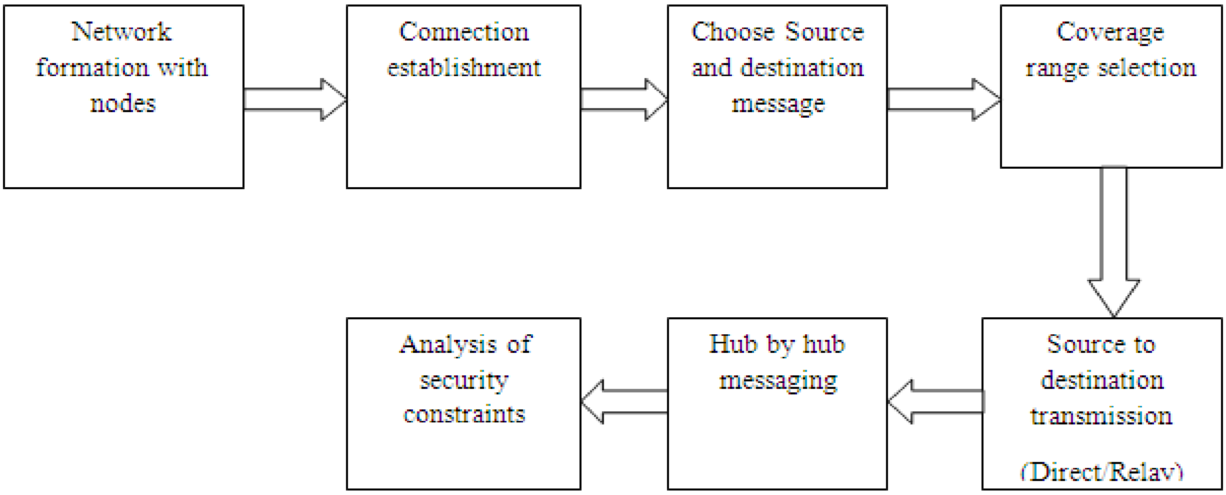

Network formation with nodes
Connection establishment
Choose Source and destination message
Coverage range selection
Source to destination transmission (Direct/Relay)
Hub by hub messaging
Analysis of security constraints

Fig.1 Block diagram for proposed system

IV. PERFORMANCE ANALYSIS FOR COLLUDING EAVESDROPPERS

For colluding eavesdropper's case, the combined received SNR at eavesdroppers from the source and the relay node *Rl* can be respectively written as

$$\varepsilon I_S = \sum E_j \in \Phi_E[\varepsilon h_{SEj}\, d^{-\alpha}{}_{S\,E}j]$$
$$\varepsilon I_{Rl} = \sum E\,{}_j \in \Phi_E[\varepsilon h_{Rl\,E\,j}\, d^{-\alpha}{}_{Rl\,E\,j}]$$

Secure connection probability

For direct transmission

$$\mathbf{P_{C\_DT}} = LI_S\,(d^{\alpha}{}_{SD})$$
$$= \mathbf{\exp\,[-Ad^2{}_{SD}]} \qquad \text{---- (1)}$$

Where $A = 2\pi\lambda E/\alpha\, \Gamma(2/\alpha)\, \Gamma[1-(2/\alpha)]$

$\Gamma(\cdot)$ is the gamma function.

$LI_S(.)$ is the laplace transform of is

For relay Transmission

$$\mathbf{P_{C\_Rl}} = L_{IS\,,IRl}(d^{\alpha}{}_{SRl},\, d^{\alpha}{}_{Rl\,D})$$
$$\mathbf{= \exp\,[-(Ad^2{}_{SD}/2) - 2Ar^2]} \quad \text{---- (2)}$$

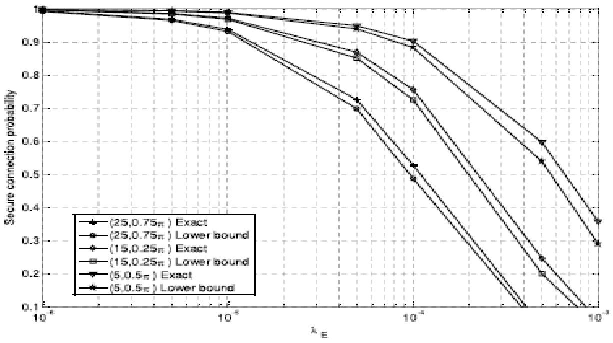


Fig. 2. Secure connection probability for colluding eavesdroppers as a function of λ_E when $\alpha = 4$, $d_{SD} = 20m$.

A. *PERFORMANCE ANALYSIS FOR NON-COLLUDING EAVESDROPPERS*

For non-colluding eavesdroppers case, the received SNR at eavesdroppers from the source and relay node *Rl*can be respectively written as

$$\varepsilon U_S = \max E\,{}_j \in \Phi_E\{\varepsilon h_{SEj} d^{-\alpha}{}_{S\,Ej}\}$$
$$\varepsilon U_{Rl} = \max E\,{}_j \in \Phi_E\{\varepsilon h_{RlEj}\, d^{-\alpha}{}_{RlEj}\}$$

B. *SECURE CONNECTION PROBABILITY*

Similar to the case of colluding eavesdroppers, the secure connection probability for direct transmission can be defined as

For direct transmission

$$\mathbf{P_{C\_DT} > \exp\,[-Ad^2{}_{SD}]} \qquad \text{---- (3)}$$

We can find that (3) is the same as (1), and it means that the secure connection probability for colluding eavesdroppers is worse than that of non colluding eavesdroppers

For relay Transmission

$$\mathbf{P_{C\_Rl} > \exp[-\,(Ad^2{}_{SD}/2) - 2Ar^2]} \quad \text{-----(4)}$$

Interestingly, we find that (4) is the same as (2). Both (3) and (4) are lower bounds of secure connection probability for non-colluding eavesdroppers, while it is obvious that the lower bound of (3) is tighter than that of (4).

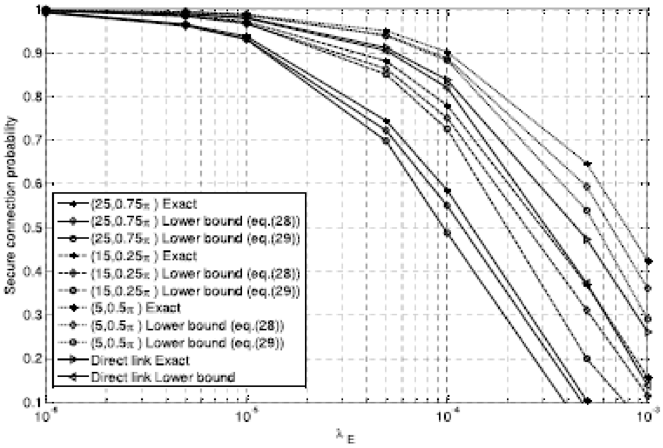
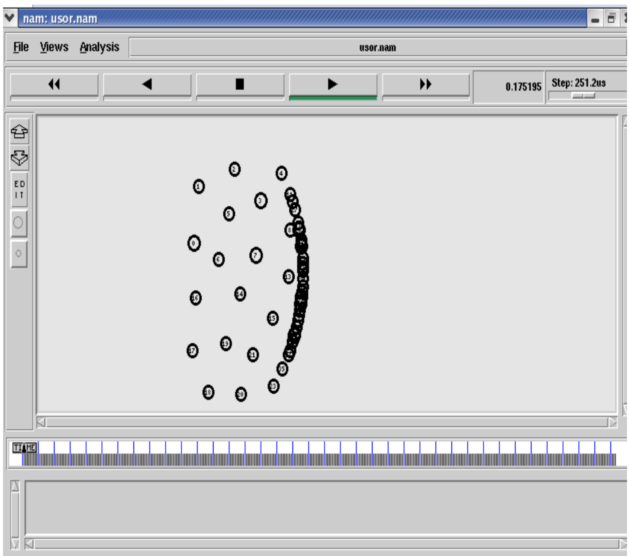


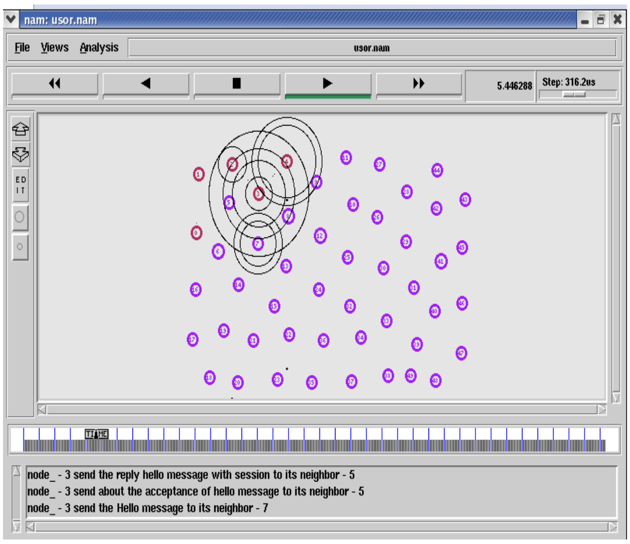
Fig. 3. Secure connection probability for non-colluding eavesdroppers as a function of λ_E when $\alpha = 4$, $d_{SD} = 20m$.

C. TECHNIQUES

Dynamic Source Routing (DSR) Techniques should used to transfer the Hub-by-Hub message transfer from Source to Destination through arbitrary relay nodes. The DSR protocol should connects the relay nodes between source and destination on Dynamic Routing strategies.DSR should select the relay node(s) based on the transmission range of base station which is chosen by the user.

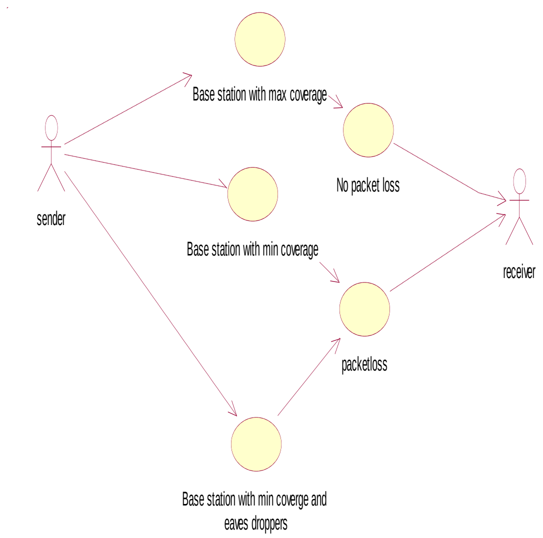
V. RESULT SNAP SHOT





```
node_ - 3 send the reply hello message with session to its neighbor - 5
node_ - 3 send about the acceptance of hello message to its neighbor - 5
node_ - 3 send the Hello message to its neighbor - 7
```

USE CASE DIAGRAM


Base station with max coverage
No packet loss
sender
Base station with min coverage
receiver
packetloss
Base station with min converge and
eaves droppers

VI. CONCLUSION AND FUTURE WORK

The results obtained from this stimulation provide useful design insights for relay networks with Security constraints. Also we can analyze when a relay transmission should provide the secure connection with small and large density of eavesdroppers in wireless adhoc network.

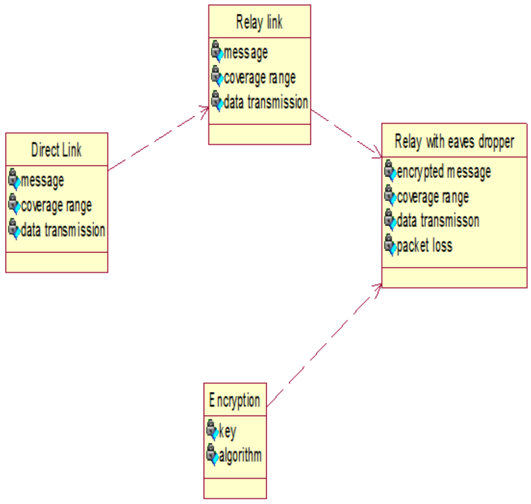
ACKNOWLEDGEMENT

I would like to thank my guide Mr.P.BRIGHT PRABAHAR Asst. Prof., Electronics and communication engineering Department, Parisutham Institute of Technology and Science, Thanjavur for his help and guidance to enable us to propose this system.

REFERENCES

[1] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8,pp. 1355–1387, Oct. 1975.
[2] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wirelessinformation-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6,pp. 2515–2534, Jun. 2008.
[3] M. Haenggi, “The secrecy graph and some of its properties,” in Proc.IEEE Int. Symp. Information Theory, Toronto, ON, Canada, Jul. 2008.
[4] P. C. Pinto, J. Barros, and M. Z. Win, “Secure communication instochastic wireless networks—Part I: Connectivity,” IEEE Trans. Inf.Forensics Security, vol. 7, no. 1, pp. 125–138, Feb. 2012.
[5] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, “ Modelinglocation uncertainty foreavesdroppers: A secrecy graph approach,”in Proc. IEEE ISIT, Austin, TX, USA, Jun. 2010, pp. 2627–2631.
[6] P. C. Pinto and M. Z. Win, “Continuum percolation in the intrinsicallysecure communications graph,” inProc. ISITA, Taichung, Taiwan, Oct.2010.

CLASS DIAGRAM



[7] X. Zhou, R. Ganti, and J. Andrews, “Secure wireless network connectivity with multi-antenna transmission,”IEEE Trans. Wireless Commun.,vol. 10, no. 2, pp. 425–430, Feb. 2011.
8] L. Lai and H. El Gamal, “The relay–eavesdropper channel: Cooperationfor secrecy,” IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019,Sep. 2008
.[9] C. Jeong and I.-M. Kim, “Optimal power allocation for secure multi-carrier relay systems,” IEEE Trans. Signal Process., vol. 59, no. 11,pp. 5428–5442, Nov. 2011.
[10] L. Dong, Z. Han, A. Petropulu, and H. Poor, “Improving wirelessphysical layer security via cooperating relays,” IEEE Trans. SignalProcess., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.